ABSTRACT

A security management system can log, investigate, respond, and track computer security incidents that can occur in a networked computer system. In other words, the security management system can produce a security record of information related to the tracking of suspicious computer activity or actual computer security threats, such as denial of service attacks or other similar compromises to computers or computer networks. The security record can include, but is not limited to, date and times of computer security incidents, a name for a particular security incident, a security management system user, and a potential source of the computer security incident. The security record can be designed as a running log that saves or records all activity of a computer incident source as well as the activity of the security team responding to the computer incident source. To produce the security record, all data that relates to a computer incident and all data that relates to a computer incident response can be sent to a separate protected database, where data is protected by digital signature algorithms (DSAs).